State of California

California Information Security Office

Incident Reporting and Response Instructions

SIMM 5340-A

(formerly SIMM 65B)

September 2013

REVISION HISTORY

REVISION	DATE OF RELEASE	OWNER	SUMMARY OF CHANGES
Initial Release	**August 2012**	**California Office of Information Security**	
Minor Update	**September 2013**	**California Information Security Office (CISO)**	**SIMM number change, transferred procedural content from State Administrative Manual (SAM), Chapter 5300**

TABLE OF CONTENTS

INTRODUCTION

State entity management must promptly investigate incidents involving loss, damage, misuse of information assets, or improper dissemination of information. All entities are required to report information security incidents in accordance with the security notification and reporting requirements in these instructions.

Proper incident management includes the formulation and adoption of a written incident management plan that provides for the timely assembly of appropriate staff that are capable of developing a response to, appropriate reporting about, and successful recovery from a variety of incidents.

In addition, incident management includes the application of lessons learned from incidents, together with the development and implementation of appropriate corrective actions directed to preventing or mitigating the risk of similar occurrences in the future.

Upon discovery of any incident that meets the notification and reporting criteria defined herein, all state entities must immediately report the incident following these Information instructions.

REPORTING CRITERIA

An incident is an occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

Incidents which must be reported to the California Highway Patrol's Emergency Notification and Tactical Alert Center (ENTAC) immediately following discovery include, but are not limited to, the following:

1. **State Data** (includes electronic, paper, or any other medium).

    a. Theft, loss, damage, unauthorized destruction, unauthorized modification, or unintentional or inappropriate release of any data classified as confidential, sensitive or personal.

    b. Possible acquisition of notice-triggering personal information by unauthorized persons, as defined in Civil Code 1798.29.

    c. Deliberate or accidental distribution or release of personal information by a state entity, or its personnel in a manner not in accordance with law or policy.

    d. Intentional non compliance by the custodian of information with his/her responsibilities.

2. **Criminal Activity** - Use of a state information asset in commission of a crime as described in the Comprehensive Computer Data Access and Fraud Act. See Penal Code Section 502.

    a. **Unauthorized Access** - This includes actions of state entity personnel and/or unauthorized individuals that involve tampering, interference, damage, or unauthorized access to state computer data and computer systems.

b. **Attacks** - This includes, but is not limited to, successful virus attacks or exploited vulnerability, web site defacements, and denial of service attacks.

3. **Equipment** – This includes theft, damage, destruction, or loss of state-owned Information Technology (IT) equipment, including laptops, tablets, integrated phones, personal digital assistants (PDA), or any electronic devices containing or storing confidential, sensitive, or personal data.

4. **Inappropriate Use –** This includes the circumventing of information security controls or misuse of a state information asset by state entity personnel and/or any unauthorized individuals for personal gain, or to engage in unauthorized peer-to-peer activity, obscene, harassing, fraudulent, illegal or other inappropriate activity

5. **Outages and Disruptions** – This includes any outage or disruption to a state entity's mission critical systems or public-facing web applications lasting more than 2-hours, or in which the incident triggers the state entity's emergency response or technology recovery.

6. **Any other incidents that violate state entity policy**.

INCIDENT NOTIFICATION

State policy requires state entities to make notification to the California Highway Patrol's Emergency Notification and Tactical Alert Center (ENTAC) immediately following discovery of an incident. Each state entity's Information Security Officer's (ISO) is responsible for notifying the proper authorities following these steps:

Responsibility of the state entity ISO or backup ISO:

Call (916) 843-4199 immediately to report the incident. This number is a 24-hour phone line at the California Highway Patrol (CHP) Emergency Notification and Tactical Alert Center (ENTAC). The CHP contact will require specific information about the incident and will forward that information to the California Information Security Office (CISO) and to the CHP Computer Crimes Investigation Unit (CCIU). Representatives from the CISO and CCIU will contact you as soon as possible following their receipt of the ENTAC notification.

IMPORTANT: A notification made to CHP or the CISO outside of the ENTAC notification process by email or other means is NOT an acceptable substitute for the required notification to ENTAC. The ISO should attempt to gather the following information before calling ENTAC; however if the information is not available, notification should not be delayed:

- Name and address of the reporting state entity
- Name, address, e-mail address, and phone number(s) of the reporting person

- Name, address, e-mail address, and phone number(s) of the ISO
- Name, address, e-mail address, and phone number(s) of the alternate contact (e.g., alternate ISO, system administrator, etc.)
- Description of the incident
- Date and time the incident occurred
- Date and time the incident was discovered
- Make / model of the affected computer(s)
- IP address of the affected computer(s)
- Assigned name of the affected computer(s)
- Operating system of the affected computer(s)
- Location of the affected computer(s)
- Actions taken prior to contacting ENTAC

Additional guidance for reporting the incident can be located on CHP's Web site at www.chp.ca.gov under "Computer Crime Reporting for State entities."

1. During this notification process, it is important to indicate if the incident involves personally identifiable information, such as notice-triggering personal information, protected health information, or electronic health information.

2. The CCIU or the CISO may contact the state entity for additional information or further investigation.

INCIDENT HANDLING AND RESPONSE

Every state shall establish and maintain in its incident management plan and procedures for ensuring incidents involving loss, damage, misuse of information assets, or improper dissemination of information are promptly investigated and for ensuring that any breach of security involving personal information, regardless of its medium (e.g., paper, electronic, verbal) are reported and handled in the most expeditious and efficient manner.

The state entity's procedures must be documented and address, at a minimum, the following:

1. **State entity Incident Response Team.**

   A state entity's procedures shall identify the positions responsible for responding to incidents and a breach of personal information. A state entity's response team must include, at a minimum, an escalation manager, the Program Manager of the program or office experiencing the incident or breach, the Information Security Officer (ISO), the Chief Privacy Officer/Coordinator (CPO) or Senior Official for Privacy, the Public Information or Communications Officer, Legal Counsel, and a representative from the CISO. The escalation manager, often the ISO or CPO, is responsible for ensuring appropriate representatives from across the organization are involved and driving the process to completion. Some incidents will require the involvement of others not mentioned above. For example, if the source of the compromised information was a computer system or database, the Chief Information Officer should also be involved in the response activity. If the incident involves unauthorized access, misuse, or other inappropriate behavior by a state employee, or the security breach involves state employee's personal information, the state entity's Personnel Officer or Human

Resource Manager should be involved. Furthermore, if the incident involves multiple state entities, the response team from each state entity may be involved.

2. **Protocol for Internal and External Communications.**

   A state entity's procedures shall outline the method, manner, and progression of internal reporting, as to ensure that executive management is informed about incidents and breaches involving personal information, and the state entity's Incident Response Team is assembled and the incident is addressed in the most expeditious and efficient manner. The state entity's procedures shall include instructions for communicating up its chain of command to Cabinet-Secretary and the Governor's Office when necessary and establishing the central point of contact for media inquiries.

3. **Protocol for Preservation of Evidence**

   The state entity's plan and procedures shall provide instruction to incident response teams and other personnel which may be involved in the response investigation of an incident for working with and through law enforcement to preserve evidence, and maintain both chain of custody and chain of evidence.

Protocol for Security Incident Reporting.

Any actual or suspected incident meeting the criteria described earlier or breach of personal information (notice-triggering and non-notice-triggering data elements) in any type of media (e.g., electronic, paper) is to be reported immediately to the CHP's ENTAC at (916) 843-4199. This telephone number is staffed 24-hours a day, seven days a week. The officers at ENTAC will require specific information about the incident and will forward that information to the CISO and to the CHP Computer Crimes Investigation Unit (CCIU). A state entity should inform the officer taking the report when immediate response assistance is needed and when the incident involves a personal information breach and the type of media involved (e.g., electronic, paper, both electronic and paper, etc.). Representatives from the CISO and CCIU will contact the state entity as soon as possible following their receipt of the ENTAC notification.

IMPORTANT: A report made to CHP, other law enforcement agencies, or the CISO outside of the ENTAC notification process by email or other means is NOT an acceptable substitute for the required report to ENTAC.

SPECIAL HANDLING INSTRUCTIONS FOR INCIDENTS INVOLVING PERSONAL INFORMATION

Decision Making Criteria and Protocol for Notifying Individuals

A state entity's procedures shall include documentation of the methods and manner for determining when and how a notification is to be made. The procedures shall be consistent with and comply with applicable laws and state policies. At a minimum, a state entity's procedures will address the following elements:

1. Whether the notification is required by law.
2. Whether the notification is required by state policy.
3. Timeliness of notification.
4. Source of notice.

5. Content of notice.
6. Approval of notice prior to release.
7. Method(s) of notification.
8. Preparation for follow-on inquiries.
9. Other actions that state entities can take to mitigate harm to individuals.
10. Other situations when notification should be considered.

A more detailed description of these elements is set forth in the Requirements to Respond to Incidents Involving a Breach of Personal Information (SIMM 5340-C, formerly SIMM 65D).

Notice to Affected Individuals

Notice to individuals when a breach of unencrypted notice-triggering data elements occurs, regardless of the media involved (electronic or paper), and in accordance with criteria set forth above.

CISO Prior Review and Approval of Breach Notice

The CISO provides review and must approve the breach notice prior to its release to any individual as set forth in Requirements to Respond to Incidents Involving a Breach of Personal Information (SIMM 5340-C).

INCIDENT REPORTING

The Information Security Incident Report (SIMM 5340-B), is available via the CISO's website at www.infosecurity.ca.gov/. The report must be submitted to the CISO within ten working days of the state entity's becoming aware of an incident involving the theft of such information, including information stolen in conjunction with the theft of a computer or data storage device.

A state entity Information Security Incident Report (SIMM 5340-B, formerly SIMM 65C) outlining the details of the incident and corrective actions to be taken must be completed and forwarded to the CISO within 10 business days following notification of the incident. The report is to contain a Plan of Action and Milestones (POAM) for each distinct vulnerability or issue which was determined to have been the root cause of the incident, based on the state entity's root cause analysis. The report is signed by the state entity's director and Information Security Officer, and when the incident involves a breach of personal information the Privacy Officer must sign the report as well.

Incident reports are to be mailed to:

California Information Security Office
P.O. Box 1810, Mail Stop Y-12
Rancho Cordova, CA 95741-1810

Further, any incident involving personal identifying information may require the state entity to notify the effected individuals and additional reporting may be necessary for state entities that must adhere to Health Insurance portability and Accountability Act (HIPAA) requirements. Refer to the California Office of Health Information Integrity (CalOHII) Policies and Procedures which can be found on the CalOHII website at http://www.ohi.ca.gov/.

The Office may require that the state entity provide additional information in conjunction with its assessment of the incident.

Questions regarding the notification or reporting process may be directed to security@state.ca.gov or by calling (916) 445-5239.